# Probleme de securitate - Platforma Autentic Monitor & Expert Monitor

"Stefan Deleanu" <office@entryrise.com>

October 17, 2022 at 10:30 PM

To: ramo@ramo.ro

Buna ziua,

Va contactez pentru a raporta urmatoarele probleme de securitate informatica, pe care le-am identificat in timpul utilizarii platformei autentic monitor oferita de catre RAMO.

Am identificat urmatoarele probleme:

- **Lipsa autentificare poze martor - Grad de risc scazut (sau comportament intentionat):** Pozele martor oferite prin intermediul platformei ExpertMonitor au un format specific, cea ce permite utilizatorilor neautorizati accesul la pozele martor, fara sa achizitioneze un abonament al RAMO.
- **Directory Listing - Grad de risc mediu:** Datorita unor probleme in sanitizarea informatiei venita din partea client-ului web al utilizatorilor, acestia pot sa obtina acces sa visualizeze intregul arbore de fisiere de pe drive-ul unde este gazduita platforma autentic monitor, prin introducerea semnelor "../" in parametrul prin care utilizatorii trimit partea si subdirectorul vizat. Desi in sine aceasta problema nu ofera unor potentiali actori maliciosi accesul la platforma, ea poate fi utilizata pentru a obtine informatii care sunt utilizate ulterior in atac, si pentru a obtine date cu caracter personal care sunt prezente in proformele generate de platforma.
- **Copii de rezerva nesecurizate - Grad de risc ridicat:** Folderul unde este gazduita aplicatia web include copii de rezerva ale platformei digitale administrate de RAMO, permitand utilizatorilor care dispun de link-ul asociat fisierul sa il descarce, fara ca autentificarea sa fie necesara. Acest fapt permite potentialilor actori maliciosi sa obtina datele de autentificare, dar si totalitatea fisierelor si codul sursa al platformei.
- **Query-uri SQL nesanitizate - Grad de risc ridicat:** Un atacator poate trimite un sir de date care sa cauzeze aplicatia sa le interpreteze ca si cum ar fi query-uri SQL trimise de catre serverul RAMO. Acest fapt poate cauza autentificarea neautorizata in conturile utilizatorilor, inclusiv in conturile de administrator ale RAMO, descarcarea fisierelor care includ date cu caracter personal.

Recomandari de natura tehnica:

- Sanitizarea tuturor query-urilor SQL.
- Blocarea accesului la copiilor de rezerva in baza unor masuri de autentificare.
- Blocarea accesului la proforme, facturi, si contracte in spatele autentificarii, astfel incat utilizatorii sa nu aiba acces si la fisierele altor terti, in special persoane fizice care pot fi interesate in achizitionarea produselor RAMO.
- Auditarea intregii platforme RAMO, pentru potentialele riscuri de securitate. (Expert Monitor & Autentic Monitor)

Pentru orice detaliu de natura tehnica, va stau la dispozitie aici, sau telefonic.

Multumesc Mult,
Deleanu Stefan-Lucian

EntryRise Logo

**Stefan-Lucian Deleanu**
Director / ENTRYRISE S.R.L

Website: www.entryrise.com
Email: office@entryrise.com
Phone: +40786833325